Claims:

1. A method for enabling the use of valid authentication certificates when the private key and public key of any of the certifying authorities have expired comprising:

   - obtaining a server certifying authority chain (SCAC) certificate by the server from the said certifying authority,

   - presenting the original valid authentication certificate along with the said server certifying authority chain certificate, by the server to the browser during the SSL handshake,

   - accepting the transaction by the browser after verification of the original authentication certificate using the expired public key of the certifying authority, and verifying the said SCAC certificate using the new public key of the said certifying authority.

2. A method as claimed in claim 1 wherein the said server certifying authority chain (SCAC) certificate is obtained by each server whenever the certifying authority invalidates its public key, by:

   - contacting the certifying authority using the server's private key for authentication,

   - verifying the request by the certifying authority using the server's public key,

   - generating the SCAC certificate by the certifying authority using its new private key and forwarding to the said server.

3. A method as claimed in claim 2 wherein the generating of the said SCAC certificate includes the authentication of the server name and the server public key, old certifying authority public key and certifying authority name.

4. A method as claimed in claim 1 wherein the certifying authority in case of client will also issue client certificates known as (CCAC) certificates, which will work the same way as (SCAC) certificates.

5. A method as claimed in claim 1 wherein during SSL handshake when the client presents its certificate, it will also present the CCAC certificate to the server.

6. In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

- a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,
- a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,,
- a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

7. A system as claimed in claim 6 wherein the said means for the server to obtain a SCAC certificate from the said certifying authority whenever the said certifying authority withdraws its public key comprising:

- a means for contacting the said certifying authority and requesting certifying authority chain certificate using the server's private key for authentication,

9

a means for verification of the request by the certifying authority,

- a means for generating and forwarding the certifying authority chain certificate to the server by the said certifying authority.

5   8.   A system as claimed in claim 6 wherein the said certifying authority have means to generate the said SCAC certificate containing authentication of the server name and the server public key, old certifying authority public key and certifying authority name.

10   9.   A system as claimed in claim 6 wherein said certifying authority have also means to issue client certificate known as (CCAC) certificates, which will work the same way as the (SCAC) certificate.

10.   A system as claimed in claim 6 wherein it includes means to present CCAC certificates to the server during SSL handshake when the client presents its certificate.

15